This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1-120 (Canceled)

121. (Currently Amended) A computer-readable medium having stored thereon a data ~~structure~~ file corresponding to a digital content package, the data structure including:

a first data field containing encrypted digital content to be rendered in accordance with a corresponding digital license, the encrypted digital content being decryptable according to a decryption key (KD) obtained from the license;

a second data field containing a content or a package ID identifying one of the digital content and the package, the corresponding license also having the content or package ID such that the content or package ID from the package is employed to locate the corresponding license; and

a third data field containing license acquisition information including a location of a license provider for providing the license after identifying the content or package ID to such license provider,

wherein the license acquisition information is in an unencrypted form;

wherein the license provider location is a network address; and

wherein the data ~~structure~~ file is provided by a content provider having a public key and a private key, the data ~~structure~~ file further including a fourth data field containing the content provider public key, the corresponding license including a content

provider digital certificate issued and signed by the content provider private key to show permission from the content provider to the license provider to provide the corresponding license, such that the content provider public key from the package is employed to validate the content provider digital certificate of the corresponding license.

122-123 (Canceled)

124. (Currently Amended) The ~~data structure~~ medium of claim 121 wherein the license provider location is an Internet address.

125. (Canceled)

126. (Currently Amended) The ~~data structure~~ medium of claim 121 wherein the content provider public key is encrypted according to the decryption key (KD).

127. (Currently Amended) The ~~data structure~~ medium of claim 126 wherein the encrypted content provider public key is signed by the content provider private key, and wherein alteration of the encrypted content provider public key prevents validation of the data ~~structure~~ file.

128. (Currently Amended) The ~~data structure~~ medium of claim 121 wherein the content provider public key is signed by the content provider private key, wherein alteration of the content provider public key prevents validation of the data ~~structure~~ file.

129. (Currently Amended) The ~~data structure~~ medium of claim 121 further comprising a ~~fourth~~ fifth data field containing a key ID identifying the decryption key (KD).

130. (Currently Amended) The ~~data structure~~ medium of claim 121 wherein the data ~~structure~~ file is provided by a content provider authorized by a root source to provide the data ~~structure~~ file, the data ~~structure~~ file further comprising a ~~fourth~~ fifth data field containing a certificate from the root source indicating that the content provider has authority from the root source to provide the data ~~structure~~ file.

131. (Currently Amended) The ~~data structure~~ medium of claim 130 wherein the content provider has a public key and a private key, and wherein the certificate includes the public key of the content provider.

132. (Currently Amended) The ~~data structure~~ medium of claim 131 wherein the root source has a public key and a private key, wherein the certificate is signed with the private key of the root source, and wherein the public key of the root source must be obtained to decrypt the encrypted signature.

133. (Currently Amended) The ~~data structure~~ medium of claim 121 wherein the data ~~structure~~ file is provided by a content provider authorized by an intermediary source to provide the data ~~structure~~ file, the intermediary source in turn being authorized by a root source to authorize the content provider, the data ~~structure~~ file further comprising a ~~fourth~~

fifth data field containing a first certificate from the root source indicating that the intermediary source has authority from the root source to authorize the content provider, and a ~~fifth~~ sixth data field containing a second certificate from the intermediary source indicating that the content provider has authority from the intermediary source to provide the data ~~structure~~ file.

134. (Currently Amended) The ~~data structure~~ medium of claim 133 wherein the content provider has a public key and a private key, wherein the intermediary source has a public key and a private key, wherein the first certificate includes the public key of the intermediary source, and wherein the second certificate includes the public key of the content provider.

135. (Currently Amended) The ~~data structure~~ medium of claim 134 wherein the root source has a public key and a private key, wherein the first certificate is signed with the private key of the root source, wherein the second certificate is signed with the private key of the intermediary source, wherein the public key of the root source must be obtained to decrypt the encrypted signature of the first certificate, and wherein the public key of the intermediary source is obtained from the first certificate to decrypt the encrypted signature of the second certificate.